Essential AI vendor evaluation: 9 critical questions you must ask

July 2024

General Disclaimer

Although Versa Networks has attempted to provide accurate information in this guide, Versa Networks does not warrant or guarantee the accuracy of the information provided herein. Versa Networks may change the programs or products mentioned at any time without prior notice. Mention of non-Versa Networks products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

At Versa, we are frequently asked to help companies navigate the complexities of adopting AI technologies. Whether it's about selecting the right AI solution, understanding its best use cases, or effectively deploying it within existing infrastructures, our discussions with customers consistently highlight several key themes. These themes, drawn from a wide range of use cases and deployments, underline the critical considerations that businesses must address to successfully leverage AI for cybersecurity. The following questions encapsulate these recurring themes and provide a structured approach to evaluating AI products, helping you make informed decisions in the complex landscape of AI-driven cybersecurity solutions.

As businesses increasingly rely on AI to help their security posture, it becomes important to ask the right questions that unearth the product's efficacy, data handling, integration with existing systems, ROI, and transparency. This set of essential questions aims to guide you through the critical aspects of evaluating AI cybersecurity solutions, ensuring that you select a product that not only meets your immediate needs but also supports long-term security objectives and operational efficiency. From understanding how AI detects cyber attacker behaviors to assessing cost implications and integration with your current security stack, these questions will help you make informed decisions in the complex landscape of AI-driven cybersecurity solutions.

1. How do you use AI to detect and stop cyberattacks?

AI has become a critical tool in cybersecurity for detecting and stopping cyberattacks. Evaluate how the AI product identifies threats, such as through anomaly detection, behavior analysis, or pattern recognition. AI systems can monitor network traffic, user behavior, and system activities to identify potential threats in real-time. Assess the product's ability to adapt to new and evolving threats, often by using machine learning models that learn from past incidents to improve detection accuracy. Consider the integration of AI with existing security infrastructure, such as firewalls, intrusion detection systems, and security information and event management (SIEM) systems. Evaluate the effectiveness of the AI product in reducing false positives and providing actionable insights. A robust AI cybersecurity solution should enhance your overall security posture, providing early warning and automated responses to mitigate the impact of cyberattacks.

2.How does your AI prioritize threats targeting high-risk hosts and accounts so analysts know what's urgent?

Effective threat prioritization is essential for efficient incident response in cybersecurity. AI can play a significant role in identifying and prioritizing threats targeting high-risk hosts and accounts. Assess how the AI product determines what constitutes a high-risk target, taking into account factors like the sensitivity of data, criticality of the host or account, and historical attack patterns. Evaluate the algorithms and criteria used for threat scoring and prioritization. Understand how the AI system alerts analysts to urgent threats and provides context for decision-making. Does the AI product integrate with existing security tools to streamline the incident response workflow? Consider the accuracy and reliability of the prioritization process and how it helps reduce alert fatigue among security teams. A robust AI solution for threat prioritization should enhance the effectiveness of your cybersecurity operations by ensuring that the most critical threats are addressed promptly and efficiently.

3. How will your AI reduce the workload for my security analysts?

Reducing the workload for security analysts is a significant benefit of using AI in cybersecurity. Assess how the AI product automates repetitive tasks, such as log analysis, threat detection, and incident response. Evaluate the AI's ability to filter out false positives and prioritize genuine threats, allowing analysts to focus on more complex and high-impact issues. Understand how the AI product provides actionable insights and context to help analysts make informed decisions quickly. Consider features like automated reporting, alerting, and workflow management that streamline the overall security process. Additionally, look into how the AI product facilitates collaboration among analysts and integrates with existing security tools. A well-designed AI solution should significantly reduce the manual workload, improve efficiency, and enhance the overall productivity of your security team.

4. How will AI help my team investigate and respond to incidents more efficiently?

AI can significantly enhance the efficiency of incident investigation and response. Evaluate how the AI product aids in quickly identifying the root cause of incidents and providing comprehensive incident analysis. Assess the product's ability to correlate data from various sources, identify patterns, and provide a detailed timeline of events. Consider how the AI product assists in automating response actions, such as isolating affected systems, blocking malicious traffic, or initiating predefined incident response

protocols. Look into the tools and features provided for collaboration and communication among team members during incident response. Additionally, evaluate the integration of AI with your existing incident response platforms and workflows. An effective AI solution should streamline the investigation process, reduce the time to resolution, and improve the overall effectiveness of your incident response efforts.

5. What data does the AI product require, and how is it collected, processed, and stored?

The success of an AI product heavily depends on the quality and quantity of data it uses. Identify the types of data required—structured or unstructured, internal or external—and how this data is collected. Notably, determine whether it collects data from across the infrastructure – from your WAN, LAN, cloud and data center.

Additionally, assess how the data is processed and stored. Look into the data preprocessing techniques employed, such as cleaning, normalization, and transformation. This has an impact on the fidelity of the conclusions and also the speed at which conclusions or information can be delivered.

6. What is the level of transparency and explainability of the AI algorithms used?

Transparency and explainability are critical for building trust in AI products. Understand how the AI algorithms work and the rationale behind their decisions. This is particularly important for applications in regulated industries like finance, healthcare, and legal, where accountability and compliance are paramount. Assess the extent to which the AI product provides explanations for its outputs. Transparent AI models allow users to understand the decision-making process, identify potential biases, and improve the model's performance over time. Look for features that deliver context for algorithmic decisions. An AI product that offers high transparency and explainability will facilitate user acceptance, regulatory compliance, and continuous improvement of the AI system.

7. How is the AI product maintained and updated, and what is the roadmap for future developments?

Continuous maintenance and updates are essential for the long-term success of an AI product. Evaluate the support and maintenance services provided by the vendor. Understand the frequency and nature of updates, including improvements in

algorithms, new features, and security patches. A clear maintenance plan ensures that the AI product remains up-to-date with the latest technological advancements and industry standards. Additionally, inquire about the vendor's roadmap for future developments. This includes planned enhancements, new functionalities, and strategic initiatives. Understanding the roadmap will help you assess whether the AI product will continue to meet your evolving needs and provide a sustainable competitive advantage. A well-maintained AI product with a robust development roadmap ensures long-term value and reliability.

8. What are the total costs of ownership, including licensing, implementation, and ongoing operational costs?

Evaluating the total cost of ownership (TCO) is crucial for understanding the financial investment required for an AI product. Consider all cost components, including licensing fees, implementation costs, customization, integration with existing systems, and ongoing operational expenses such as maintenance, support, and updates. Compare these costs with the projected benefits and return on investment (ROI) to ensure the AI product provides value for money. Be aware of any hidden costs or potential price escalations over time. Understanding the TCO helps in budget planning and financial forecasting, ensuring that the AI product is a viable and sustainable investment for your organization. A clear understanding of costs will enable you to make informed financial decisions and achieve the desired outcomes from the AI implementation.

9. How will your AI solution integrate with my current security stack?

Integration with your current security stack is critical for the effective deployment of any AI solution. Assess how the AI product will work with your existing security tools, such as firewalls, intrusion detection/prevention systems, security information and event management (SIEM) systems, and endpoint protection platforms. Determine the ease of integration and whether the AI solution provides out-of-the-box connectors or requires custom development. Evaluate the compatibility with your existing infrastructure, including cloud environments, on-premises systems, and hybrid setups. Understand how data will be shared and synchronized between the AI solution and your current security tools. Consider the impact on your existing workflows and whether the AI solution will enhance or disrupt current processes. A well-integrated AI solution should seamlessly augment your existing security capabilities, providing enhanced visibility, improved threat detection, and streamlined incident response.

Learn more at www.versa-networks.com
Follow us @versanetworks.

2550 Great America Way, Suite 350 | Santa Clara, CA | 95054